WHAT IS CLAIMED IS:

1. A system for providing quarantine on a network comprising:

a client seeking access to a network resource;

a first server for providing the client with a manifest of checks that, if passed by the client, establish that the client possesses a required configuration; and

a second server for providing access to the network resource, wherein the second server denies the client access to the network resource until the client presents proof that the client possesses the required configuration.

2. The system of claim 1, wherein the checks include at least one of checks for installed software, a software version, an installed patch, an installed anti-virus system, an anti-virus state, a firewall state, an installed service, file sharing, a registry value, a registry key, and a file system state.

3. The system of claim 1, wherein the client comprises delegates that perform the checks in the manifest of checks.

4. The system of claim 1, wherein the client sends the first server a result the checks, and the first server provides the client with a certificate certifying that the client possesses the required configuration if the client passes the checks, and stores a copy of the certificate in a database.

5. The system of claim 4, wherein the client presents the certificate to the second server, and the second server validates the certificate by comparing the certificate to the copy of the certificate which is obtained from the first server.

6. The system of claim 1, wherein if the client fails the checks, the first server instructs a user of the client how to correct a problem causing the client to fail the checks.

7. The system of claim 1, wherein if the client cannot provide proof that the client possesses the required configuration, the second server directs the client to the first server.

8. The system of claim 1, wherein the client sends the first server a result the checks, and the first server generates a certificate certifying that the client possesses the required configuration if the client passes the checks, and stores the certificate in a first database along with a unique identifier of the manifest of checks.

9. The system of claim 8, wherein the second server includes a second database that is a replica of the first database, wherein the client proves possession of the required configuration by sending the second server the unique identifier, wherein the second server compares the unique identifier to the unique identifier stored with the certificate in the second database.

10. The system of claim 1, wherein the first server requests a software inventory from the client and provides the client software necessary for the required configuration.

11. The system of claim 1, further comprising an access point for mediating communication between the client and the second server, wherein the second server is protected by a firewall.

12. The system of claim 1, wherein the first server is a service executing on a computing device and the second server is a service also executing on the computing device.

13. A method for a client to acquire access to a network resource, comprising:

receiving a manifest of checks from a first server, wherein the checks determine whether the client possesses a required configuration;

performing the checks in the manifest of checks and sending the results of the checks to the first server;

requesting access to the network resource from a second server controlling access to the network resource; and

sending proof of the required configuration to the second server.

14. The method of claim 13, further comprising:

receiving a request for a software inventory from the first server;

receiving software necessary for the required configuration; and

installing the software.

15. The method of claim 13, further comprising:

sending results of the checks to the first server; and

receiving a certificate certifying that the client possesses a valid configuration.

16. The method of claim 15, further comprising presenting the certificate to the second server as proof of the required configuration.

17. The method of claim 13, wherein the proof is a unique identifier for the manifest.

18. The method of claim 13, wherein the first server is a service executing on a computing device and the second server is a service also executing on the computing device.

19. A method for provisioning a client with a required configuration, comprising:

sending a manifest of checks to the client, wherein the checks determine whether the client possesses a required configuration;

receiving a result of the checks; and

if the client passes the checks,

generating a certificate certifying that the client possesses the required configuration,

storing the certificate in a database, and

making the certificate accessible to a server controlling network access to network resource.

20. The method of claim 19, further comprising, if the client fails the checks, instructing a user of the client to correct a flaw causing the failure.

21. The method of claim 19, further comprising providing the certificate to the client.

22. The method of claim 19, further comprising:

requesting a software inventory from the client;

receiving the software inventory from the client; and

sending the client software necessary for the required configuration.

23. A method for quarantining a client from access to a network resource, comprising:

receiving a request for access to the network resource from the client;

receiving proof of a required configuration;

validating the proof by comparing the proof to information obtained from a trusted server;

if the proof is valid, allowing access to the network resource; and

if the proof is invalid, denying access to the network resource.

24. The method of claim 23, further comprising, if the proof is invalid, directing the

client to the trusted server so that the required configuration is obtained.

25. The method of claim 23, wherein the proof is a certificate, obtained from the trusted server, certifying that the client has the required configuration.

26. The method of claim 23, wherein the proof is a unique identifier for a manifest of checks that the client has performed.

27. A data structure representing a certificate issued for a computer indicating that computer possesses a required configuration, comprising:

a creation time;

an expiration time;

a unique identifier; and

a manifest number indicating a manifest of checks that were performed on the computer, wherein the certificate was issued after the checks were passed.